IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
BUTTE DIVISION

Linda Pierce, Nathan Thomas, Latosha Austin, Natasha McIntosh, Debby Worley, Valerie Lozoya, Jolinda Murphy, Lauren Neve, Molly O'Hara, Roscoe Eldridge, LaVonne Madden, Susie Garcia, and Gilbert Criswell, Plaintiffs, v. Snowflake, Inc., Defendant.	Case No. CV-25-17-BU-BMM

PLAINTIFFS' CLASS ACTION COMPLAINT

INTRODUCTION

1. Data companies are acutely aware of the critical importance of cybersecurity in an increasingly interconnected world. With the exponential growth of cloud storage, companies are entrusted with sensitive information, ranging from personal details to financial records.

2. This is a "hub-and-spoke" data breach case brought on behalf of Plaintiffs against the "hub" of the data breach. The "hub" in this case is Defendant Snowflake, which is a company that specializes in cloud-storage technologies to warehouse and secure sensitive data, and in selling data storage and analytics products. Snowflake sells its data storage services to numerous companies, or "spokes," who store information on Snowflake's data cloud. These spokes[1] included Ticketmaster, Advance Auto Parts, LendingTree, and AT&T.

[1] The Defendant in this class action complaint is Snowflake, Inc. ("Snowflake"). This complaint is filed for jurisdictional purposes for transfer to an MDL against Snowflake and other entities, including Ticketmaster, LLC and Live Nation Entertainment, Inc. (referred to collectively as "Ticketmaster"); Advance Auto Parts, Inc. and Advance Stores Company, Inc. (referred to collectively as "Advance Auto"); LendingTree, LLC, and Quotewizard.com, LLC (referred to collectively as "LendingTree"); and AT&T, Inc. and AT&T Mobility, LLC (referred to collectively as "AT&T"). The non-Snowflake entities are referred to herein as "Spokes."

3. Stressing to investors that it built its data-storage product "with security as a core tenet,"[2] Snowflake has long understood and acknowledged the importance of robust cybersecurity to protect consumer data.

4. Similarly, the Spokes have also long understood the importance of robust cybersecurity, as discussed herein, to protect the data of their own customers, employees, and subscribers—information from which Spokes, themselves, extract a handsome profit. The Spokes include Fortune 500 corporations and have a collective market capitalization totaling hundreds of billions of dollars.

5. Information security policies and practices are imperative to ensure that sensitive information is not exposed to unauthorized third parties. These exposures, commonly referred to as "data breaches," can cause significant harm to individuals—exposing them to fraud and attempted fraud, identity theft, reputational harm, and the continuing risk of harm that results from criminals having their sensitive information.

6. A single data breach can result in catastrophic consequences for individuals. As a result, and based upon legal and industry-standard requirements, companies prioritize robust cybersecurity measures.

---

[2] Snowflake Inc. 2024 Annual Report (Form 10-K) at 15 (Mar. 26, 2024) ("Snowflake 2024 10-K"), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001640147/264ea0e0-8e73-4f07-9f54-78ab341a2c79.pdf.

7. In this case, however, Snowflake did not implement three of the most basic and industry-standard cybersecurity policies to protect Personal Information, including most prominently, multifactor authentication (MFA).[3] The foreseeable result: a massive data breach (the "Data Breach"). The cybercriminal group known by codename UNC5537 used compromised login credentials for the Spokes, plugged them in to Spokes' Snowflake accounts, and successfully exfiltrated Personal Information belonging to hundreds of millions of consumers.

8. UNC5537's success was made possible by basic data security failings on the part of Snowflake and the Spokes. These companies collectively flouted relevant governmental guidance, regulations, statutes, and industry standards.

9. The Data Breach's foreseeable consequences are neither imaginary nor hypothetical: shortly after the Data Breach, sensitive information previously stored with Snowflake began appearing for sale on the dark web.[4]

---

[3] "Personal Information," as used herein, refers to that information which was exposed to cybercriminals through the Data Breach. While the information exposed varies from each Spoke Defendant, each protected that information behind credentials (i.e., a username and password), intending that it would not be exposed to unauthorized third parties. As alleged herein, inadequate, negligent, and reckless cybersecurity practices resulted in that information being exposed.

[4] Snowflake Breach Threat Actor Offers Data of Cloud Company's Customers, SOCRadar, https://socradar.io/overview-of-the-snowflake-breach/ (last accessed Jan. 13, 2025).

10. Plaintiffs and Class Members[5] now face the real and actual harm that the Data Breach has caused them and will continue to cause them. Not only have cybercriminals obtained valuable and sensitive Personal Information about them, but that information has been obtained by other criminals and offered for resale to still more criminals. As a result, Plaintiffs and Class Members have already experienced fraud or attempted fraud, an invasion of their privacy, time and expenses spent mitigating the imminent and substantial risk of data misuse, and are at significant risk of identity theft, reputational harm, and other injuries.

PARTIES

I. Defendant

11. **Snowflake Inc.** is a cloud-based data storage company incorporated under Delaware law, with its principal place of business located at 106 E. Babcock Street, Suite 3A, Bozeman, Montana.[6]

II. Plaintiffs

12. **Plaintiff Susie Garcia** is a citizen of California residing in Riverside. Plaintiff Garcia has been a customer of Ticketmaster for over 10 years and last purchased a ticket in April 2023, when she provided Ticketmaster with her name, address, email, phone number, and credit card information. She does not

---

[5] "Class Members" refers to those individuals who were impacted by the Data Breach, as alleged herein.

[6] Snowflake Inc. 2024 10-K at 1.

remember logging into her Ticketmaster account after this date. Since the Data Breach, Plaintiff Garcia has experienced injury related to her Personal Information.

13. **Plaintiff Valerie Lozoya** is a citizen of California residing in Hawthorne. Plaintiff Lozoya received a data breach notice letter, via U.S. mail, directly from Ticketmaster, dated July 17, 2024. Plaintiff Lozoya is a current customer of Ticketmaster and has regularly purchased tickets. In doing so, she provided Ticketmaster with at least her name, address, email, phone number, and payment card information. Since the Data Breach, Plaintiff Lozoya has experienced injury related to her Personal Information

14. **Plaintiff LaVonne Madden** is a citizen of Montana residing in Shepherd. Plaintiff Madden received a data breach notice letter, via U.S. mail, directly from Ticketmaster in July 2024. Plaintiff Madden is a former customer of Ticketmaster, and believes she last purchased a ticket in 2008 and in doing so, provided Ticketmaster with at least her name, address, email, phone number, and payment card information. Since the Data Breach, Plaintiff Madden has experienced injury related to her Personal Information.

15. **Plaintiff Jolinda Murphy** is a citizen of Montana residing in Missoula. Plaintiff Murphy received a data breach notice letter, via U.S. mail, directly from Ticketmaster, dated July 17, 2024. Plaintiff Murphy is a customer of

Ticketmaster, but she cannot recall the last time she purchased tickets. She does recall that, when she did purchase tickets, she provided Ticketmaster with at least her name, address, email, phone number, and payment card information. Since the Data Breach, Plaintiff Murphy has experienced injury related to her Personal Information.

16. **Plaintiff Lauren Neve** is a citizen of California residing in San Juan Capistrano. Plaintiff Neve is a former customer of Ticketmaster, where she last purchased a ticket in 2022 and in doing so, provided Ticketmaster with at least her name, address, email, and payment card information. Since the Data Breach, Plaintiff Neve has experienced injury related to her Personal Information.

17. **Plaintiff Molly O'Hara** is a citizen of Massachusetts residing in Revere. Plaintiff O'Hara received a data breach notice letter, via U.S. mail, directly from Ticketmaster, dated July 9, 2024. Plaintiff O'Hara is a current customer of Ticketmaster who has regularly purchased tickets. In doing so, she provided Ticketmaster with at least her name, address, email, phone number, and payment card information. Since the Data Breach, Plaintiff O'Hara has experienced injury related to her Personal Information.

18. **Plaintiff Linda Pierce** is a citizen of Texas residing in Jacksonville. Plaintiff Pierce received a data breach notice letter, via U.S. mail, directly from QuoteWizard, dated July 30, 2024. Plaintiff Pierce recalls applying for a loan

through a LendingTree web-based application in the past 1-2 years and in so doing, provided LendingTree with at least her name, home address, email address, phone number, date of birth, driver's license number, Social Security number, and financial information. Since the Data Breach, Plaintiff Pierce has experienced injury related to her Personal Information.

19. **Plaintiff Nathan Thomas** is a citizen of Washington residing in Bellingham, Washington. Plaintiff N. Thomas is a frequent user of LendingTree and received a notice letter from QuoteWizard dated July 30, 2024. In order to utilize services from LendingTree, Plaintiff N. Thomas provided LendingTree with his name, address, email address, phone number, and date of birth. Since the Data Breach, Plaintiff Thomas has experienced injury related to his Personal Information.

20. **Plaintiff Latosha Austin** is a citizen of California residing in Fresno. Plaintiff Austin is a current AT&T customer and has been a customer since 2000. Plaintiff Austin was also a customer of Cricket Wireless in or around 1999-2000. Plaintiff Austin received correspondence from AT&T in or around June 2024. Since the Data Breach, Plaintiff Austin has experienced injury related to her Personal Information.

21. **Plaintiff Gilbert Criswell** is a citizen of California residing in San Francisco. Plaintiff Criswell is a current customer of AT&T and has been using its

services for approximately 10 years. In or around September 2024, Plaintiff Criswell received a notification from Google Security that his account information and password were compromised by AT&T, prompting him to change his password. Since the Data Breach, Plaintiff Criswell has experienced injury related to his Personal Information.

22. **Plaintiff Roscoe Eldridge** is a citizen of Illinois residing in South Beloit. Plaintiff Eldridge is not a customer of AT&T, Cricket Wireless, or AT&T's MVNOs. He does frequently communicate with individuals who use those phone carriers, however, and did so throughout 2022. For example, his daughter has had a Cricket Wireless account for over a decade, and he was in frequent contact with her through phone calls and texts throughout 2022. Since the Data Breach, Plaintiff Eldridge has experienced injury related to his Personal Information.

23. **Plaintiff Natasha McIntosh** is a citizen of Alabama residing in Brockton. Plaintiff McIntosh was a customer of Boost Mobile from 2002 to 2022 and was an employee of Boost Mobile for a year, starting around 2003. She provided Boost Mobile with at least her name, SSN, email, and payment card information. Since the Data Breach, Plaintiff McIntosh has experienced injury related to her Personal Information.

24. **Plaintiff Debby Worley** is a citizen of New Jersey residing in Clifton. Plaintiff Worley has been a Boost Mobile customer for approximately two

to three years. Boost Mobile is an MVNO of AT&T and its customers, like Plaintiff Worley, suffered from the Data Breach in part as a result of Boost Mobile's use of AT&T's network. Since the Data Breach, Plaintiff Worley has experienced injury related to her Personal Information.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00) and is a class action in which Plaintiffs are citizens of states different from Defendant.

26. This Court has personal jurisdiction over Snowflake because its principal place of business is located in Montana.

27. Venue properly lies in this judicial district because, it is the district in which Defendant has the most significant contacts.

FACTUAL ALLEGATIONS

28. Snowflake is one of the largest data storage providers in the United States and it contracts with thousands of organizations around the world to securely store their consumer and employee data on its "Data Cloud" platform.[7] Snowflake's

[7] Snowflake, *How It All Started*, https://www.snowflake.com/en/company/overview/about-snowflake/ (last visited Jan. 6, 2025).

platform is a product and a service that provides companies the ability to store, process, and analyze large volumes of consumer and employee data.[8]

29. Snowflake's product is typically referred to as "Software as a Service" (SaaS), which refers to the fact that Snowflake's software allows its customers to connect to cloud-based applications over the internet.

30. Each of the Spokes is a Snowflake customer and stores consumer and/or employee Personal Information on the Data Cloud.

31. Snowflake is aware and understands that data security is a key feature of the data storage services that it provides to its customers. The following examples illustrate how Snowflake's marketing highlights the strength of its data security practices as a selling point to its customers:

- Snowflake maintains a "Security Hub" webpage that centralizes updates relating to data security. The header of the Security Hub website provides: "Security has been foundational to the Snowflake platform since the very beginning. Our robust security features help you protect your data so you can achieve the results you need."[9]

- The Security Hub website also includes the following quote from Brad Jones, Snowflake's Chief Information Security Officer ("CISO"), emphasizing Snowflake's "industry-leading" data security policies: "Since our founding in 2012, the security of our

---

[8] Snowflake, *The Snowflake Platform*, https://www.snowflake.com/en/data-cloud/platform/ (last visited Jan. 6, 2025).

[9] Snowflake, *Snowflake Security Hub*, https://www.snowflake.com/en/resources/learn/snowflake-security-hub/ (last visited Jan. 6, 2025).

> customers' data has been our highest priority. This unwavering commitment is why we're continuously strengthening our industry-leading, built-in security policies to deliver a trusted experience for our customers. To foster ongoing transparency, we will regularly update this page with the latest security information."[10]

- Snowflake also maintains a "Securing Snowflake" website that provides customers with data security guidance. The website represents, "Snowflake provides industry-leading features that ensure the highest levels of security for your account and users, as well as all the data you store in Snowflake."[11]

32. Snowflake is also well aware of industry guidance and regulations that set standards for effective data security practices. Snowflake's marketing repeatedly advertises that its "industry-leading" data security practices enable companies comply with relevant data security standards and regulations.

33. For example, on a webpage titled "Data Security Compliance: Protecting Sensitive Data" (the "Data Security Compliance website"), Snowflake represents: "Snowflake helps organizations streamline security compliance, providing the tools and support required to meet regulatory compliance standards.

---

[10] *Id.*

[11] Snowflake, *Securing Snowflake*, https://docs.snowflake.com/en/guides-overview-secure (last visited Jan. 6, 2025).

With industry-leading data security and governance features, organizations can shift their focus from protecting their data to analyzing it."[12]

34. On the Data Security Compliance website, Snowflake further represents how its services enable customers to comply with relevant industry standards and regulations, touting that its services afford customers "[b]aked-in government and industry data security compliance" and allow for "comprehensive compliance, security and privacy controls that are universally enforced." For example, in a section titled, "How Snowflake Supports Security Compliance," Snowflake represents the following[13]:

- "**Baked-in government and industry data security compliance.** Snowflake has achieved numerous government and industry data security compliance credentials, validating the high level of security required by industries, as well as state and federal governments. Snowflake's government deployments have achieved Federal Risk and Authorization Management Program (FedRAMP) Authorization to Operate (ATO) at the Moderate level along, and support a range of compliance standards: International Traffic in Arms Regulations (ITAR), System and Organization Controls 2 (SOC 2) Type II, PCI DSS and Health Information Trust Alliance (HITRUST)."

- "**Universal governance.** Inconsistent governance policies across systems and users can introduce security risk to your data. Snowflake's single governance model provides comprehensive compliance, security and privacy controls that are universally

---

12 Snowflake, *Data Security Compliance: Protecting Sensitive Data*, https://www.snowflake.com/trending/data-security-compliance/ (last visited Jan. 6, 2025).

13 *Id.*

> enforced. Snowflake Horizon unifies and extends data governance resources. With Snowflake Horizon, data teams, data governors and data stewards can leverage a built-in, unified set of compliance, security, privacy, interoperability and access capabilities in the AI Data Cloud. Snowflake Horizon provides the toolkit required to protect and audit data, apps and models with data quality monitoring and lineage. And advanced privacy policies and data clean rooms allow organizations to tap into the full value of their most sensitive data."

35. As one of the nation's largest cloud storage data providers, Snowflake knew or should have known about the importance of implementing effective data security practices to protect Personal Information stored on the Data Cloud, particularly because it held itself out as doing exactly that.

36. Indeed, cloud storage databases are prime targets for cybercriminals due to the sheer volume of data they house. One recent report has highlighted the risks presented by cloud storage as follows[14]:

> It is estimated that more than 60% of the world's corporate data is stored in the cloud. That makes the cloud a very attractive target for hackers. In 2023, over 80% of data breaches involved data stored in the cloud. That is not just because the cloud is an attractive target. In many cases, it is also an easy target due to cloud misconfiguration – that is, companies unintentionally misuse the cloud, such as allowing excessively permissive cloud access, having unrestricted ports, and use unsecured backups

[14] Stuart Madnick, *Why Data Breaches Spiked in 2023*, Harv. Bus. Rev. (Feb. 19, 2024), https://hbr.org/2024/02/why-data-breaches-spiked-in-2023.

Multiple, basic cybersecurity failures led to the Data Breach.[15]

37. The events leading up to the Data Breach and its fallout are summarized in a June 10, 2024 report published by Mandiant (the "Mandiant Report"), a cybersecurity firm that assisted Snowflake in its investigation of the Data Breach.[16]

38. Beginning on or around April 2024, a cybercriminal group named UNC5537 carried out a successful cyberattack on Snowflake, exfiltrating the data of hundreds of Snowflake customers, including the Spokes.

39. UNC5537 is a known cybercriminal group likely comprised of hackers in North America. A financially motivated threat actor, UNC5537 employs information-stealing malware to infiltrate systems, collect user data, exfiltrate that

---

[15] Additional details regarding the breach will be revealed through discovery, including information related to a report prepared by another, reputable cybersecurity company, which was demanded to be taken off the internet by Snowflake. *See* Part Two, *infra*.

[16] Mandiant, *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*, Google Cloud (June 10, 2024), https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion (cited to hereinafter as "*Mandiant Report*"). Since Snowflake had a hand in the *Mandiant Report*, the events are likely worse than presented, and will be clarified in discovery. *See also Snowflake Breach: Hacker Confirms Access Through Infostealer Infection*, Hudson Rock, https://archive.is/tljkW ("Hudson Rock Report," archived website).

data, and then sell it on underground cybercrime forums or sell the information to other hackers.[17]

40. UNC5537's successful cyberattack on Snowflake and the Spokes was simple and easily prevented. As the Mandiant Report put it, the cyberattack was "not the result of any particularly novel or sophisticated tool, technique, or procedure" but was the consequence of "missed opportunities" on the part of Snowflake and the Spokes to properly secure their credentials.[18]

41. UNC5537's cyberattack boiled down to two basic steps. First, UNC5537 gained access to a customer's Snowflake credentials—i.e., their username and password. Stolen credentials are common and represent a well-known and easily anticipated risk by cybersecurity companies.[19] According to the Mandiant Report, UNC5537 was also "likely able to aggregate credentials" for a large number Snowflake customers by simply perusing various sources of

---

17 UNC5537 Summary, Mphasis (June 17, 2024), https://www.mphasis.com/content/dam/mphasis-com/global/en/home/services/cybersecurity/june-17-19-unc5537.pdf.

18 *Mandiant Report*, *supra*.

19 *See* TJ Alldridge, *Stolen Credentials Make You Question Who Really Has Access*, Mandiant (Feb. 13, 2024), https://cloud.google.com/blog/products/identity-security/stolen-credentials-make-you-question-who-really-has-access ("stolen credentials are the third most used infection vector behind exploits and phishing").

previously stolen credentials, as "large lists of stolen credentials exist both for free and for purchase inside and outside of the dark web."[20]

42. Next, UNC5537 simply used the stolen credentials to login to a Snowflake customer's account and exfiltrate customer data.[21]

43. According to the Mandiant Report, the success of UNC5537's straightforward cyberattack was made possible by "three primary factors" on the part of Snowflake and the Spokes.[22]

44. **First**, the affected customers did not have MFA enabled, nor did Snowflake require them to have it enabled. MFA is a basic and industry-standard cybersecurity measure, available for nearly three decades,[23] that requires a user to, in addition to providing their username and password, further authenticate their identity through another source, such as through a passcode sent by text message or

---

20 *Mandiant Report*, *supra.*

21 *Id.*

22 *See also* Brad Jones, Detecting and Preventing Unauthorized User Access, Snowflake (June 2, 2024), Detecting and Preventing Unauthorized User Access - Cybersecurity - Snowflake (Snowflake recommending MFA, trusted locations, and resetting credentials).

23 Bojan Šimić, *Identity in the Digital Age and the Rise of Multi-Factor Verification*, Forbes (Oct. 10, 2024), https://www.forbes.com/councils/forbestechcouncil/2024/10/10/identity-in-the-digital-age-and-the-rise-of-multi-factor-verification/ (MFA was developed by AT&T as a system to exchange codes on two-way pagers).

email.[24] Without MFA, a valid username and password was all UNC5537 needed to access a Snowflake customer's data—similar to a key placed under a doormat.

45. Strikingly, even though the federal government has urged companies to use MFA to secure data since 2016,[25] and Snowflake offered "free and available" MFA to customers since June 2015,[26] at the time of the Data Breach, Snowflake's default setting turned off MFA. Moreover, Snowflake customers did not have the ability to require their users to use MFA.

46. Snowflake later changed these policies, but not until after the Data Breach. On July 9, 2024, Snowflake announced that customers could now enforce MFA for its users and monitor MFA compliance.[27] And on September 13, 2024, Snowflake announced a new policy which, for the first time, established a default

---

[24] Rose de Fremery, *Tracing the Evolution of Multi-Factor Authentication*, LastPass (Oct. 16, 2023), https://blog.lastpass.com/posts/tracing-the-evolution-of-multi-factor-authentication.

[25] *Fact Sheet:* Cybersecurity National Action Plan, The White House (Feb. 9, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[26] Snowflake Advances Cybersecurity Excellence by Joining CISA Secure by Design Pledge (July 29, 2024), https://www.snowflake.com/en/blog/snowflake-cybersecurity-cisa-secure-by-design/. Snowflake has also used MFA to protect its own systems. Mihir Bagwe, *The Snowballing of the Snowflake Breach: All About the Massive Snowflake Data Breach*, CyberExpress (June 17, 2024), https://thecyberexpress.com/all-about-massive-snowflake-breach/.

[27] Brad Jones & Anoosh Saboori, *Snowflake Admins Can Now Enforce Mandatory MFA*, Snowflake (July 9, 2024), https://www.snowflake.com/en/blog/snowflake-admins-enforce-mandatory-mfa/.

setting *requiring* MFA for users of Snowflake accounts created as of October 2024.[28]

47. **Second,** Snowflake did not have policies and procedures in place to rotate or disable stale credentials. Notably, many of the credentials stolen by UNC5537 through malware were old, and were originally stolen through various malware attacks dating as far back to 2020. But without policies in place to rotate or disable such stale credentials, the years-old credentials remained valid and allowed UNC5537 to exfiltrate Snowflake customers' data.

48. Addressing the issue of stolen credentials, Snowflake now advertises that it automatically disables leaked passwords detected on the dark web.[29]

49. **Third,** the affected customers—including the Spokes—did not restrict access to Snowflake cloud-based storage based upon certain trusted locations. Conditional Access Policies allow companies to fine-tune access to control from which devices and locations users can access resources. Again, without such

---

[28] Anoosh Saboori & Brad Jones, *Snowflake Strengthens Security with Default Multi-Factor Authentication and Stronger Password Policies*, Snowflake (Sept. 13, 2024), https://www.snowflake.com/en/blog/multi-factor-identification-default/.

[29] Snowflake Will Automatically Disable Leaked Passwords Detected on the Dark Web, Snowflake (Nov. 14, 2024), https://www.snowflake.com/en/blog/leaked-password-protection/.

protection, a valid username and password entered was all UNC5537 needed to access a Snowflake customer's data from anywhere at any time.

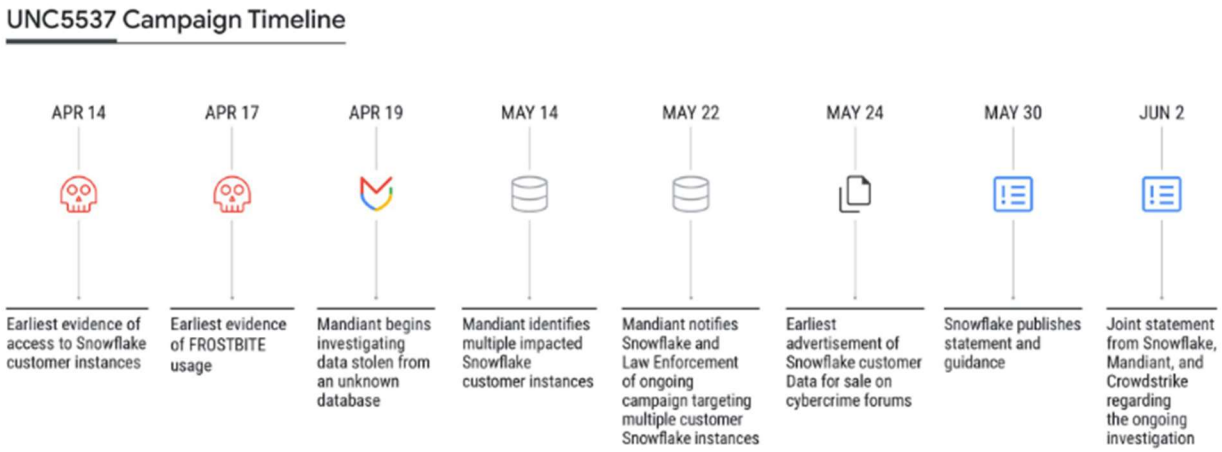
50. On May 30, 2024, Snowflake publicly disclosed the Data Breach for the first time through a blog post authored by CISO Brad Jones, which explained that Snowflake "became aware of potentially unauthorized access to certain customer accounts on May 23, 2024" and was "investigating an increase in cyber threat activity targeting some of our customers' accounts."[30]

51. The Mandiant Report documented the timeline of the Data Breach, which shows a concerning lag in Snowflake's response. As shown in the Mandiant Report timeline provided below, Snowflake did not make a public statement regarding the Data Breach until May 30, 2024. Snowflake's public disclosure came over a month and a half after Mandiant identified evidence of improper access to Snowflake customer data on April 14—but only a week after advertisements for the sale of stolen Snowflake customer data started showing up on cybercrime forums on May 24.[31]

---

30 Brad Jones, *Detecting and Preventing Unauthorized User Access*, Snowflake (May 30, 2024), https://snowflake.discourse.group/t/detecting-and-preventing-unauthorized-user-access/8967.

31 *Mandiant Report*, *supra*.



52. The Mandiant Report further found that UNC5537 was operating "with the intent of data theft and extortion" and was "advertising victim data for sale on cybercrime forums and attempting to extort many of the [customer] victims."[32]

53. As set out in more detail herein, Plaintiffs' and Class Members' Personal Information has already been sold and exchanged on the dark web between UNC5537 and various other cybercriminal threat actors such as Scattered Spider.[33]

54. The Mandiant Report concluded that UNC5537's cyberattack "underscores the urgent need for credential monitoring, the universal enforcement of MFA and secure authentication, limiting traffic to trusted locations for crown

---

32 *Id.*

33 SC Staff, *Ransom demands issued to Snowflake hack victims*, SC Media (June 18, 2024), https://www.scworld.com/brief/ransom-demands-issued-to-snowflake-hack-victims.

jewels, and alerting on abnormal access attempts."[34] Credential monitoring, MFA, limiting access, and alerts are all ubiquitous cybersecurity practices that have been standard for years.

Relevant industry standards and regulations for data security were not followed by Snowflake.[35]

55. The Federal Trade Commission ("FTC") has issued guidance and taken enforcement actions that together illustrate the data security industry standards applicable to Snowflake and the Spokes.

56. Indeed, the FTC's enforcement actions have established that a company's failure to maintain reasonable and appropriate data security of consumer Personal Information violates the FTC Act's prohibition on "unfair or deceptive acts."[36]

---

34 *Mandiant Report*, *supra.*

35 The below recitation of information security standards only provides an introduction as to applicable guidance. *See, e.g.,* NIST Update: Multi-Factor Authentication and SP 800-63 Digital Identity Guidelines, Federal Cybersecurity and Privacy Forum (Feb. 15, 2022), https://csrc.nist.gov/csrc/media/Presentations/2022/multi-factor-authentication-and-sp-800-63-digital/images-media/Federal_Cybersecurity_and_Privacy_Forum_15Feb2022_NIST_Update_Multi-Factor_Authentication_and_SP800-63_Digital_Identity_%20Guidelines.pdf.

36 *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 244-47 (3d Cir. 2015); Isabella Wright and Maia Hamin, *"Reasonable" Cybersecurity in Forty-Seven Cases: The Federal Trade Commission's Enforcement Actions Against Unfair and Deceptive Cyber Practices*, DFR Lab (June 12, 2024), https://dfrlab.org/2024/06/12/forty-seven-cases-ftc-cyber/.

57. In 2016, the FTC published guidance titled, *Protecting Personal Information: A Guide for Business* (the "FTC 2016 Guidance").[37] The FTC 2016 Guidance:

- Stresses the importance of "[c]ontrol[ling] access to sensitive information" and expressly encourages businesses to "[c]onsider using multi-factor authentication, such as requiring the use of a password and a code sent by different methods."[38]
- Emphasizes that companies should respond appropriately when credentials are compromised, providing that businesses should "[r]equire password changes when appropriate—for example, following a breach."[39]
- Instructs companies to restrict data access privileges by "[s]cal[ing] down access to data" and ensuring that "each employee should have access only to those resources needed to do their particular job."[40]
- Warns companies that their data security practices depend on their personnel, which "includ[e] contractors" and encourages companies to "investigate [contractor] data security practices and compare their standards" and "verify compliance" with written security expectations.[41]
- Recommends companies encrypt information stored on computer networks, understand their network's vulnerabilities,

---

37 *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business ("The FTC 2016 Guidance").

38 *Id.* at 13.

39 *Id.*

40 *Id.* at 7.

41 *Id.* at 27.

and implement policies to correct any security problems and respond to security incidents.[42]

- Advises companies not to maintain Personal Information longer than necessary, not to collect more Personal Information than necessary, to use industry-tested methods for data security, and monitor and respond to suspicious activity.[43]

58. In 2021, the FTC amended its "Safeguards Rule" that applies to financial institutions, including retailers that issue their own credit card to consumers and companies that bring together buyers and sellers of products and services.[44] The Safeguard Rule requires covered businesses to "[i]mplement multi-factor authentication for anyone accessing customer information on [the business's] system," to "[i]mplement and periodically review access controls [to] [d]etermine who has access to customer information and reconsider on a regular basis whether they still have a legitimate business need for it," and to "[i]mplement procedures and controls to monitor when authorized users are accessing customer information on your system and detect unauthorized access."[45]

---

42 *Id.* at 9-11.

43 *Id.* at 6-22.

44 FTC Safeguards Rule, 86 Fed. Reg. 707272-01, 70305-06 (Dec. 9, 2021) (to be codified at 16 C.F.R. § 314.2(h)(2)(i), (xiii)).

45 *FTC Safeguards Rule: What Your Business Needs to Know*, Fed. Trade Comm'n, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited Jan. 7, 2025).

59. In February 2023, the FTC published an article titled, *Security Principles: Addressing underlying causes of risk in complex systems.* The article highlighted the importance of MFA, stating: "Multi-factor authentication is widely regarded as a critical security practice because it means a compromised password alone is not enough to take over someone's account."[46]

60. The FTC's enforcement actions over the past five years further emphasize the critical and fundamental role MFA plays in an effective data security system, where the FTC has repeatedly obtained MFA as a form of injunctive relief in data security enforcement actions.[47]

61. The FTC has also issued guidance for businesses regarding how to respond to data breaches, titled *Data Breach Response: A Guide for Business* (the "FTC Response Guidance"). The FTC Response Guidance stresses the importance of providing individuals affected by a data breach with notice, explaining: "If you quickly notify people that their personal information has been compromised, they

---

[46] Alex Gaynor, *Security Principles: Addressing underlying causes of risk in complex systems*, Fed. Trade Comm'n (Feb. 1, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems.

[47] *FTC v. Equifax, Inc.*, No. 1:19-CV-03297, 15 (N.D. Ga. July 23, 2019) (Stipulated Order); *In re Chegg, Inc.*, 2023151 FTC C-4782, 5 (Jan. 25, 2023) (Order); *In re Drizly, LLC*, 2023185 FTC C-4780, 6 (Jan. 9, 2023) (Order).

can take steps to reduce the chance that their information will be misused."[48] The guidance emphasizes that businesses should "[c]learly describe what you know about the compromise" and include "what information was taken." Notifying individuals as to the type of information that was compromised in the breach provides key information that allows them to "take steps to limit the damage."[49]

62. Specific to cloud-storage applications, in June 2020, the FTC published an article titled, *Six steps toward more secure cloud computing.* The article warned, "[a]s cloud computing has become business as usual for many businesses, frequent news reports about data breaches and other missteps should make companies think carefully about how they secure their data." The article expressly highlights the importance of MFA in protecting consumer data stored on cloud services, recommending that businesses: "Require multi-factor authentication and strong passwords to protect against the risk of unauthorized access."[50]

---

48 *Data Breach Response: A Guide for Business*, Fed. Trade Comm'n (Feb. 2021), https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business ("FTC Response Guidance").

49 *Id.*

50 Elisa Jillson & Andy Hasty, *Six steps toward more secure cloud computing*, Fed. Trade Comm'n (June 15, 2020), https://www.ftc.gov/business-guidance/blog/2020/06/six-steps-toward-more-secure-cloud-computing.

63. In March 2023, the FTC issued a Request for Information seeking public comment on "Business Practices of Cloud Computing Providers that Could Impact Competition and Data Security."[51] After reviewing over 100 public comments on the issue, the FTC published a report in November 2023 titled, *Cloud Computing RFI: What we heard and learned.*[52] The report expressly flagged the room for improvement in cloud security as follows: "[A] a number of commenters argued there is a great deal of room for improvement in cloud security; that default security configurations could be better; and that the 'shared responsibility' model for cloud security often lacks clarity, which can lead to situations where neither the cloud provider nor the cloud customer implements necessary safeguards."[53]

The Data Breach harmed Plaintiffs and Class Members.

64. The effects of the Data Breach were felt immediately—not only by Snowflake and the Spokes—but by individual consumers. Personal Information is

---

51 *Solicitation for Public Comments on the Business Practices of Cloud Computing Providers*, Fed. Trade Comm'n (Mar. 22, 2023), https://www.regulations.gov/docket/FTC-2023-0028/document.

52 Nick Jones, *Cloud Computing RFI: What we heard and learned*, Fed. Trade Comm'n (Nov. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/11/cloud-computing-rfi-what-we-heard-learned.

53 *Id.* Snowflake used this "shared responsibility" model. *What We Know So Far about the Snowflake "Breach,"* Symmetry Systems (Nov. 6, 2024), https://www.symmetry-systems.com/blog/what-we-know-so-far-about-the-snowflake-breach/ ("Despite the high-profile nature of the breaches and the potential reputational risk, Snowflake has not deviated from the shared responsibility model.").

valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" to corporations in America.[54]

65. Criminal law also recognizes the value of Personal Information and the serious nature of the theft of Personal Information by imposing prison sentences for its theft. This strong deterrence is necessary because cybercriminals extract substantial revenue through the theft and sale of Personal Information. Once a cybercriminal has unlawfully acquired Personal Information, the criminal can use the Personal Information to commit fraud or identity theft or sell the Personal Information to other cybercriminals on the black market.

66. Information protected by credentials—usernames and passwords—is intended to stay private, and not to be disclosed to third parties (otherwise, why password-protect the information, at all?). But because of Snowflake's failure to follow basic cybersecurity guidelines, the information stored on Snowflake's cloud-based servers was accessible to cybercriminals, who exfiltrated the data for nefarious purposes.

---

[54] Illustratively, Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of $182.5 billion and net income of $40.2 billion. $160.7 billion of this revenue derived from its Google business, which is driven almost exclusively by leveraging the Personal Information it collects about users of its various free products and services. Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

67. Each of the Spokes has disclosed that certain types of Personal Information were exposed in the Data Breach. They include, at a minimum:

- **Advance Auto**: Information collected from individuals as part of the employment application process, including Social Security numbers, driver's license or other government issued identification numbers, and dates of birth.[55]
- **Ticketmaster**: consumer name, contact information, and encrypted credit card information.[56]
- **LendingTree**: customer contact information (names and addresses), driver's license number.[57]
- **AT&T**: records of calls and text of nearly all of AT&T's cellular customers, customers of other companies using AT&T's wireless network, and AT&T's landline customers who interacted with cellular numbers between May 1, 2022 and October 31, 2022. The information also contains records from January 2, 2023, for a small number of customers.[58]

68. The Personal Information exposed is extremely valuable and can be used for a number of nefarious purposes.

---

[55] Advance Stores Company, Incorporated, Notice of Data Breach (July 10, 2024), https://consumer.sc.gov/sites/consumer/files/Documents/Security%20Breach%20Notices/AdvanceStoresCompanyInc.pdf ("Advance Auto Notice").

[56] Ticketmaster Data Security Incident, https://help.ticketmaster.com/hc/en-us/articles/26110487861137-Ticketmaster-Data-Security-Incident.

[57] QuoteWizard Notice of Data Breach (July 30, 2024) ("QuoteWizard Notice"), https://ago.vermont.gov/sites/ago/files/documents/2024-08-09%20QuoteWizard%20Data%20Breach%20Notice%20to%20Consumers.pdf.

[58] AT&T Addresses Illegal Download of Customer Data, AT&T (July 12, 2024) ("AT&T Notice"), https://about.att.com/story/2024/addressing-illegal-download.html.

A. Sale of the Snowflake information on the dark web and to other criminals.

69. First, cybercriminals have already confirmed the stolen Personal Information's value by selling the data on the dark web and to other cybercriminals.

70. Some dark web sites are simply places for people who wish to avoid tracking while browsing the internet.[59] However, the anonymity of the dark web has led to the creation of a number of markets and forums which traffic in illegal merchandise and content, including stolen Personal Information.[60]

71. The dark web is a heavily cloaked part of the internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and Personal Information. Websites appear and disappear quickly, making it a dynamic environment.

---

[59] Thomas J. Holt, *Open, Deep, and Dark: Differentiating the Parts of the Internet Used For Cybercrime*, Mich. State Univ., https://cj.msu.edu/_assets/pdfs/cina/CINA-White_Papers-Holt_Open_Deep_Dark.PDF (last visited Nov. 26, 2024).

[60] *Crime and the Deep Web*, Stevenson Univ., https://www.stevenson.edu/online/about-us/news/crime-deep-web/ (last visited Nov. 26, 2024); *Defending Against Malicious Cyber Activity Originating from Tor*, CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-183a (last updated Aug. 2, 2021).

72. Once stolen Personal Information is posted on the dark web, it will most likely be distributed or sold to multiple different groups and individuals, each of which can use that information for fraud and identity theft.[61]

73. When data is stolen, it can appear on the dark web across the world. In 2015, researchers created a list of 1,568 phony names, Social Security numbers, credit card numbers, addresses, and phone numbers, rolled them in an Excel spreadsheet, and then "watermarked" it with their code that silently tracks any access to the file.[62] The data was quickly spread across five continents: North America, Asia, Europe, Africa, and South America. In the end, it was downloaded by 47 different parties. It was mainly downloaded by users in Nigeria, Russia, and

---

[61] *The Dark Web and Cybercrime*, HHS (July 23, 2020), https://www.hhs.gov/sites/default/files/dark-web-and-cybercrime.pdf; Lawrence Abrams, *Scam PSA: Ransomware gangs don't always delete stolen data when paid*, BleepingComputer (Nov. 4, 2020), https://www.bleepingcomputer.com/news/security/scam-psa-ransomware-gangs-dont-always-delete-stolen-data-when-paid/.

[62] Kelly Jackson Higgins, *What Happens When Personal Information Hits The Dark Web*, DARKREADING (Apr. 7, 2015), https://www.darkreading.com/cyberattacks-data-breaches/what-happens-when-personal-information-hits-the-dark-web; Kristin Finklea, *Dark Web*, Nat'l Sec. Archive (July 7, 2015), https://nsarchive.gwu.edu/media/21394/ocr; *Dark Web*, Congressional Research Service, https://crsreports.congress.gov/product/pdf/R/R44101 (last updated Mar. 10, 2017).

Brazil, with the most activity coming from Nigeria and Russia.[63] This experiment demonstrated that data released on the dark web will quickly spread around the world.

74. Information from this Data Breach has already been found in several places on the dark web—even reappearing after law enforcement agencies shut down certain websites offering information for sale.[64]

75. In a hub-and-spoke breach such as this one, when information from one "spoke" defendant appears on the dark web, it is likely that information from other entities is likely to follow or has already been sold.

76. The information found for sale on the dark web is just the tip of the iceberg. The dark web poses significant challenges to cyber security professionals and law enforcement agencies. The dark web is legal to access and operate, and it has some legitimate applications and sites. But its hidden nature and its employment

---

[63] Pierluigi Paganini, *HOW FAR DO STOLEN DATA GET IN THE DEEP WEB AFTER A BREACH?*, Security Affairs (Apr. 12, 2015), https://securityaffairs.com/35902/cyber-crime/propagation-data-deep-web.html.

[64] *See, e.g.*, Ionut Arghire, *Hackers Boast Ticketmaster Breach on Relaunched BreachForums*, SecurityWeek (May 31, 2024), https://www.securityweek.com/hackers-boast-ticketmaster-breach-on-relaunched-breachforums/; Sergiu Gatlan, *Advance Auto Parts stolen data for sale after Snowflake attack*, Bleeping Computer (June 5, 2024), https://www.bleepingcomputer.com/news/security/advance-auto-parts-stolen-data-for-sale-after-snowflake-attack/.

of multi-level encryption make detecting and monitoring illegal activity difficult. Unlike the clear web, dark web sites do not advertise their existence.

B. There are long-lasting impacts of the Data Breach.

77. The U.S. Government Accountability Office (GAO) released a report in 2007 regarding data breaches, finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[65]

78. The GAO Report explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[66]

---

65 Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf.

66 *Id*.

79. Identity thieves use Personal Information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[67] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to, among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; or use the victim's information in the event of arrest or court action.[68]

80. With access to an individual's Personal Information, criminals can commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security number to obtain government benefits; filing a

---

[67] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things: "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[68] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Private Information and How Can You Protect Yourself*, Experian (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

fraudulent tax return using the victim's information; or committing healthcare fraud using an individual's identification. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[69]

81. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[70]

82. Theft of Social Security numbers creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new Social Security number, a breach victim has to demonstrate ongoing harm from misuse of their Social Security number, and a new Social Security number will not be provided until after the harm has already been suffered by the victim.

83. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other data (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. Data security researcher Tom Stickley, who is employed by companies to find flaws in

---

69 *Id.*

70 *Id.*

their computer systems, stated: "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[71]

84. A Data Breach does not need to expose Social Security numbers in order to expose victims to actual or concrete harm. For example, there have been numerous examples of victims of "SIM swap" fraud, where criminals essentially "take over" a victim's cell phone number in order to obtain that victim's text messages, break into the victim's accounts, and empty their life's savings. Some criminals have been able to successfully commit a SIM swap with only a victim's name and cellular number. Cellular companies do not necessarily put extra precautions in place to protect individuals from SIM-swap attacks—requiring consumers to understand the risk that such leaked information causes and request a special passcode on their accounts for additional protection.[72]

---

[71] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, Time (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[72] Donie O' Sullivan, *One man lost his life savings in a SIM hack. Here's how you can try to protect yourself*, CNN (Mar. 13, 2020), https://www.cnn.com/2020/03/13/tech/sim-hack-million-dollars/index.html; *FBI warns of growing SIM-swapping threat*, Honolulu Star-Advertiser (Feb. 9, 2022), https://www.yahoo.com/news/fbi-warns-growing-sim-swapping-061700104.html; *UPDATE: Secure Your Number to Reduce SIM Swap Scams*, AT&T, https://www.research.att.com/sites/cyberaware/ni/blog/sim_swap.html (last accessed Jan. 14, 2024); TJ Porter, *Why Sim Swapping Scams Are On The Rise And How You Can Stay Safe*, Investopedia (Dec. 16, 2024), https://www.investopedia.com/protect-yourself-from-sim-swapping-8756219; Dean Reilly, *A Deep Dive into the Tactics Used by Fraudsters*, Hacker Desk

85. Beyond SIM-swap scams, hackers can sell call log information for individuals, exposing sensitive information related to who they have called and when. Indeed, hackers attempted to post call log information from the Data Breach for President Donald Trump and Vice President Kamala Harris.[73] Exposed call records can expose individuals to harassment, identity theft, and other fraud.[74]

86. Recent reports suggest that detailed call logs can also be used to more effectively train malicious artificial intelligence (AI) models to help these models learn specific patterns of communication and movement. By analyzing communication patterns, this AI can craft highly personalized phishing messages that are more likely to succeed, especially if it can identify the parties involved and the nature of the relationship.[75]

(Aug. 4, 2023), https://hackerdesk.com/unmasking-the-sim-swap-scam-a-deep-dive-into-the-tactics-used-by-fraudsters.

[73] Jessica Lyons, *US Army soldier who allegedly stole Trump's AT&T call logs arrested*, The Register (Jan. 1, 2025), https://www.msn.com/en-us/news/crime/us-army-soldier-who-allegedly-stole-trumps-at-t-call-logs-arrested/ar-AA1wNlhv.

[74] Amanda Hetler, *AT&T data breach: What's next for affected customers?*, TechTarget (Jul. 24, 2024), https://www.techtarget.com/WhatIs/feature/ATT-data-breach-Whats-next-for-affected-customers.

[75] David Michael Berry, *How Data Breaches Empower Malicious AI: The AT&T Case Study*, Berry Networks (July 16, 2024), https://berry-networks.com/2024/07/16/how-data-breaches-empower-malicious-ai-the-att-case-study/.

87. Hackers can also use information related to a customer's prior purchase history to perpetrate phishing attacks and scams by sending existing customers fake order confirmations to steal additional personal and financial information.[76]

88. Exposed driver's license numbers are sold on the dark web because they can be used to create counterfeit licenses, open financial accounts, cash counterfeit checks, and even obtain medical care using someone's identity.[77]

89. Exposed gift cards can result in their balances being reduced to nothing—a real and serious loss of monetary value.[78] Individuals may also experience theft of their event tickets.[79]

---

[76] *See, e.g.*, *How to avoid scams impersonating Amazon this holiday season*, Amazon (Nov. 17, 2022), https://www.aboutamazon.in/news/amazon-india-news/how-to-avoid-scams-impersonating-amazon-this-holiday-season; *How to Recognize and Avoid Phishing Scams*, FTC (Sept. 2022), https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

[77] *How driver's licenses exposed in data breaches increase your risk of identity fraud*, IDX (May 6, 2021), https://www.idx.us/knowledge-center/how-drivers-licenses-exposed-in-data-breaches-increase-your-risk-of-identity-fraud; John Egan, *What Should I Do if My Driver's License Number Is Stolen*, Experian (June 13, 2024), https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

[78] Jackie Callaway, *Beware: Hackers can steal money off gift cards before you have a chance to use them*, ABC News Tampa Bay (Dec. 29, 2020), https://www.abcactionnews.com/money/consumer/taking-action-for-you/beware-hackers-can-steal-money-off-gift-cards-before-you-have-a-chance-to-use-them.

[79] Taylor O'Bier, *Hackers allegedly leak tickets from Ticketmaster to Talyor Swift tour and more*, Scripps (Jul. 10, 2024),

90. Each additional piece of Personal Information exposed in a data breach increases an individual's risk of identity fraud and exposure to scams. Information from one breach may be combined with information from other breaches to create "fullz"—or complete information about an individual sufficient to facilitate identity theft, allow for the purchase of goods and services on the internet, and enable criminals to open new accounts in a victim's name.[80]

91. Data breaches also have a deep, psychological impact on their victims. A cyberattack can feel like the digital equivalent of getting robbed, with a corresponding wave of anxiety and dread. Anxiety, panic, fear, and frustration—even intense anger—are common emotional responses when experiencing a

---

https://www.scrippsnews.com/science-and-tech/data-privacy-and-cybersecurity/hackers-allegedly-leak-tickets-from-ticketmaster-to-taylor-swift-tour-and-more ("Sp1d3rHunters hit back, stating in another forum post that the ticket information they allegedly stole was for physical ticket types and therefore they can't be refreshed. If this is true, Ticketmaster would have to void and reissue all the stolen tickets.").

[80] Robert Lemos, *All about your 'fullz' and how hackers turn your personal data into dollars*, PCWorld (June 2, 2016), https://www.pcworld.com/article/414992/all-about-your-fullz-and-how-hackers-turn-your-personal-data-into-dollars.html; Paige Tester, *What are Fullz? How Hackers & Fraudsters Obtain & Use Fullz*, DataDome (Mar. 3, 2023), https://datadome.co/guides/account-takeover/what-are-fullz-how-do-fullz-work/.

cyberattack. While expected, these emotions can paralyze the victim and prolong or worsen the consequences of a cyberattack.[81]

92. The information exposed in this Data Breach will result in actual and imminent harm for Plaintiffs and Class Members for years to come.

C. The data breach forces Plaintiffs and Class Members to take additional steps to mitigate harm.

93. In addition to all the other immediate consequences of the Data Breach, Plaintiffs and Class Members face a substantially increased risk of identity theft and fraud.

94. The FTC recommends that identity theft victims take several steps to protect their Personal Information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[82]

---

[81] Amber Steel, *The Psychological Impact of Cyber Attacks*, LastPass (Aug. 17, 2022), https://blog.lastpass.com/posts/the-psychological-impact-of-cyber-attacks. *See also* Christina Ianzito, *Identity Fraud Cost Americans $43 Billion in 2023*, AARP (Apr. 10, 2024) ("[I]n 2023, 16 percent of identity fraud victims said they'd thought about ending their lives.").

[82] *Identity Theft Recovery Steps*, FTC, https://www.identitytheft.gov/Steps (last visited Nov. 26, 2024).

95. As discussed above, cybercriminals use stolen Personal Information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

96. Studies by the Identity Theft Resource Center ("ITRC") show the multitude of harms caused by fraudulent use of personal and financial information, including needing to request government assistance, borrowing money, using savings to pay for expenses, being unable to qualify for home loans, losing a home or place of residence, being unable to care for one's family, losing an employment opportunity, missing time from work, and needing to take time off of school.[83]

97. Moreover, the harms of identity theft are not limited to the affected individual and may adversely impact other associated persons and support systems, including government assistance programs. In the ITRC study, nearly a quarter of survey respondents had to request government assistance because of identity theft, such as welfare, EBT, food stamps, or similar support systems.[84] The ITRC study concludes that identity theft victimization has an extreme and adverse effect on each

---

[83] Jason Steele, *Credit Card and ID Theft Statistics*, Creditcards.com (June 11, 2021), https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/; *see also* Identity Theft Resource Center 2023 Consumer Impact Report (Aug. 2023), https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf.

[84] *Id.*

individual as well as on all of the support systems and people associated with the individual.[85]

98. Personal Information is such an inherently valuable[86] commodity to identity thieves that, once it is compromised, criminals often trade the information on the cyber black-market for years.

99. Accordingly, there may also be a substantial lag time between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the GAO Report: "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[87]

---

85 *Id.*

86 *See, e.g.*, John T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 1, 2 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.").

87 Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf.

100. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind (e.g., purchase history or call log history), directly and materially increase the chance that a potential victim is targeted by a spear phishing attack in the future, and spear phishing results in a high rate of identity theft, fraud, and extortion.[88]

101. It would be unreasonable for individuals to wait to experience fraud or identity theft before they take steps to protect themselves from fraud or identity theft because of Snowflake's negligence or recklessness.

102. The intent of hackers is clear when they hack systems, such as the Snowflake's: they are attempting to access consumers' Personal Information for malicious purposes, such as selling it for a profit.

---

[88] *See* Leo Kelion & Joe Tidy, *National Trust joins victims of Blackbaud hack*, BBC News (July 30, 2020), https://www.bbc.com/news/technology-53567699 (concluding that personal information such as "names, titles, telephone numbers, email addresses, mailing addresses, dates of birth, and, more importantly, donor information such as donation dates, donation amounts, giving capacity, philanthropic interests, and other donor profile information . . . . in the hands of fraudsters, [makes consumers] particularly susceptible to spear phishing—a fraudulent email to specific targets while purporting to be a trusted sender, with the aim of convincing victims to hand over information or money or infecting devices with malware").

103. On average, it takes approximately three months for a consumer to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[89]

104. In addition, there is a strong probability that much of the information stolen in the Data Breach has not yet been made available on the dark web in a coherent, organized fashion, meaning Plaintiffs and Class Members will remain at an increased risk of fraud and identity theft for many years into the future. Plaintiffs and Class Members must vigilantly monitor their financial accounts, online presence, profiles, and other places where their Personal Information may appear for many years to come.

105. Purchasing monitoring products or spending additional time to monitor their Personal Information is a reasonable step to mitigate the risk of harm that Plaintiffs and Class Members face.

D. Damages can compensate victims for the harm caused by the attack.

106. The Personal Information exposed in the Data Breach has real value, as explained above. Plaintiffs and the Class Members have therefore been deprived

[89] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

of their rights to the control of that property and have lost the value they might otherwise have incurred from that data.[90]

107. Plaintiffs and the Class Members have spent significant time, and will spend more, monitoring their accounts, changing login credentials, and recovering from the inevitable fraud and identity theft which will occur, which deserves to be compensated: Snowflake has not made apportionment for this very real injury.[91]

108. Similarly, Snowflake has offered no compensation for the aggravation, agitation, anxiety, anguish, loss of dignity, intrinsic harm, and emotional distress that Plaintiffs and the Class Members have suffered, and will continue to suffer, as a result of the Data Breach: the knowledge that their information is out in the open, available for sale and exploitation at any time in the future is a real harm that also deserves compensation.

109. Plaintiffs have suffered injuries in numerous ways, including:

- Loss of economic value of their personal information, in that it has been misused for purposes to which they did not consent, and they have not been properly compensated for this misuse;

---

[90] Ravi Sen, *Here's how much your personal information is worth to cybercriminals – and what they do with it*, PBS (May 14, 2021, 12:04 PM), https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it.

[91] Time spent monitoring accounts is another common and cognizable, compensated harm in data breach cases. *See Equifax Data Breach Settlement*, FTC, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (last visited Nov. 26, 2024).

- Loss of the privacy of their personal information which has been stolen by cybercriminals and therefore already exposed to the eyes of unauthorized third parties without Plaintiffs' authorization or consent;

- Loss of the intrinsic value of their personal information and the accompanying aggravation, agitation, anxiety, anguish, loss of dignity, and emotional distress;

- Actual or attempted fraud, misuse, or identity theft caused by the Data Breach, including, but not limited to, their information being published to the clear, deep, and dark web; as well as

- Time and expenses that were reasonably spent to mitigate the impact of the breach.

110. Several Plaintiffs have already experienced actual or attempted fraud, which is reasonably related to the Data Breach, which demonstrates that the Data Breach has put them at immediate risk for additional harm.

111. The fraud and attempted fraud that certain Plaintiffs have suffered is sufficiently related to the Data Breach because of the time frame in which it occurred (after the Data Breach), and because the same information that was exposed in the Data Breach would have been used to effectuate the fraud and identity theft.

112. The harm already suffered by Plaintiffs demonstrates that the risk of harm is ongoing for all Plaintiffs and all Class Members.

Snowflake had a duty to safeguard Plaintiffs' and Class Members' information.

113. Snowflake exists because companies need a company to safeguard their information. The Personal Information of Plaintiffs and Class Members was stored on Snowflake's Data Cloud at the time of the Data Breach by a Spoke Defendant, with whom Snowflake maintained a business relationship to provide data cloud storage services.

114. Snowflake owed a common law duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information in Snowflake's possession from being compromised, accessed, stolen, or misused by unauthorized parties.

115. Snowflake's duty of reasonable care is consistent with nature of its business, which is to provide secure cloud data services and store massive amounts of data, including Plaintiffs' and Class Members' Personal Information. Snowflake had a duty to exercise reasonable care in safeguarding Plaintiffs' and Class Members' Personal Information, as it was reasonably foreseeable that the failure to do so would cause them injury.

116. Snowflake's duty of reasonable care is established by governmental regulations and industry guidance establishing industry standards for data security to safeguard Personal Information stored on cloud platforms.

117. Snowflake's duty of reasonable care is established by its own marketing statements, which hold out its cloud services as providing "built-in," "baked-in," and otherwise turnkey data security compliance systems.

Snowflake breached its duty and engaged in unfair trade practices.

118. Snowflake breached its duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Personal Information by failing to implement adequate data security practices, which caused the Data Breach.

119. Snowflake is well aware of the fact that it is a high-value target for cybercriminals. In March 2023, the FTC sought comments from Computing Providers (like Snowflake) and their impact on end users, customers, companies, and other businesses across the economy (like Spokes) on the business practices of cloud computing providers including issues related to the market power of these companies, impact on competition, and potential security risks.[92]

120. Despite industry guidance at the time of the Data Breach, while Snowflake permitted customers to use MFA, it required customers to opt in. It did not require MFA, including for specific users in customer environments.

---

[92] Press Release, Fed. Trade Comm'n, *FTC Seeks Comment on Business Practices of Cloud Computing Providers that Could Impact Competition and Data Security* (March 22, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-seeks-comment-business-practices-cloud-computing-providers-could-impact-competition-data (last visited Aug. 20, 2024).

Additionally, Snowflake did not provide customers with the ability to enforce MFA on its users—i.e., require users to use MFA.

121. A prominent cybersecurity firm executive described the practical failings of Snowflake's MFA configuration as follows[93]:

> MFA is a critical component in protecting against identity theft, and specifically against attacks related to the successful theft of passwords through phishing, malware (infostealers), or leakage of reused passwords from compromised sites.
>
> While Snowflake offers users the ability to turn on MFA, this is a feature that is not enabled on users by default and … it cannot be enforced on users by the admin of the tenant. This means Snowflake leaves it up to every user to decide whether they want to enroll with MFA or not. This naturally leads to many Snowflake users not having MFA turned on.
>
> Most SaaS vendors, once deployed as an enterprise solution, allow administrators to enforce MFA … they require every user to enroll in MFA when they first login and make it no longer possible for users to work without it.

122. It was feasible at the time of the Data Breach for Snowflake to allow customers to enforce MFA across their userbase. Indeed, on July 9, 2024—less than a month after disclosing the Data Breach—Snowflake rolled out a "new option" to "help admins enforce usage of MFA" by "requir[ing] MFA for all users in an

---

93 Shane Snider, *Snowflake's Lack of MFA Control Leaves Companies Vulnerable, Experts Say*, Information Week (June 5, 2024), https://www.informationweek.com/cyber-resilience/snowflake-s-lack-of-mfa-control-leaves-companies-vulnerable-experts-say.

account." In the announcement, Snowflake touted the enforcement of MFA as a "[b]est practice[]."[94]

123. It was also feasible at the time of the Data Breach for Snowflake to turn on MFA by default, instead of having it turned off. On September 13, 2024—just three months after disclosing the Data Breach—Snowflake rolled out another new policy enforcing MFA by default on accounts created as of October 2024.[95]

124. In addition, many of the compromised credentials used by UNC5537 were old and had been acquired from malware campaigns dating back to 2020. Snowflake could have closed off this vulnerability by requiring customers to regularly update their credentials, notifying customers to rotate their credentials accordingly, or monitoring info stealer marketplaces for compromised credentials and blocking access by those credentials (something Snowflake now does).

125. Snowflake also could have prevented the Data Breach by maintaining intrusion detection and prevention systems that notify customers of unusual network traffic, such as a login made by a suspicious credential that could be

---

[94] Brad Jones and Anoosh Saboori, *Snowflake Admins Can Now Enforce Mandatory MFA*, Snowflake (Jul. 9, 2024), https://www.snowflake.com/en/blog/snowflake-admins-enforce-mandatory-mfa/.

[95] Anoosh Saboori & Brad Jones, *Snowflake Strengthens Security with Default Multi-Factor Authentication and Stronger Password Policies*, Snowflake (Sept. 13, 2024), https://www.snowflake.com/en/blog/multi-factor-identification-default/.

identified by its last login date. Such a system would be consistent with the PCI Cloud Computing Guidelines, which provides, "Since customer access to low level network traffic is impossible, it must rely on Providers for IDS/IPS, monitoring and alerting."[96]

126. Snowflake, through these data security failings, was negligent and breached its duty to Plaintiffs and Class Members to protect their Personal Information—information which it knew was sensitive—stored on Snowflake's Data Cloud.

127. Snowflake's breach of its duty proximately caused the Data Breach. Had Snowflake maintained adequate data security practices (such as requiring or allowing customers to require MFA, credential rotation, or intrusion detection), the Data Breach would have been prevented.

128. Snowflake's data security failings also constitute an unfair trade practice because of its failure to maintain reasonable and appropriate data security.

129. Rather than take responsibility for its actions, Snowflake foisted the blame and responsibility onto the Spokes to "query for unusual activity and conduct further analysis to prevent unauthorized user access."[97]

---

96 *PCI SSC Cloud Computing Guidelines*, *supra* at 63.

97 Alert, *Snowflake Recommends Customers Take Steps to Prevent Unauthorized Access*, CISA (June 3, 2024), https://www.cisa.gov/news-

130. Even after the Data Breach, Snowflake insists that it was not breached. Despite failing to implement many basic cybersecurity measures, which could have prevented the Data Breach, and despite adopted a "shared responsibility" model, Snowflake insisted that it was not responsible. Snowflake's CEO Sridhar Ramaswamy's representation to its investors was, "[a]s extensively reported, the issue wasn't on the Snowflake side. . . . After multiple investigations by internal and external cybersecurity experts, we found no evidence that our platform was breached or compromised."[98]

131. Snowflake refuses to take responsibility for its failure to implement basic cybersecurity policies and protocols which would have prevented the Data Breach, even though it has implemented several of those policies since the breach occurred.

132. But the details set forth in the Mandiant Report are not the only cybersecurity failings of Snowflake. The threat actor was also able to sign in through Snowflake's ServiceNow account using stolen Snowflake credentials,

---

events/alerts/2024/06/03/snowflake-recommends-customers-take-steps-prevent-unauthorized-access.

[98] Matt Kapko, *After a wave of attacks, Snowflake insists security burden rests with customers*, CybersecurityDive (Aug. 22, 2024), https://www.cybersecuritydive.com/news/snowflake-security-responsibility-customers/724994/.

bypassing Snowflake's identity and access management platform, which provided single sign-on capabilities for Snowflake.[99]

133. It was reported that the threat actor was able to exfiltrate massive amounts of data from Snowflake corresponding to hundreds of companies.[100]

134. Hudson Rock first reported the intrusion by the threat actor into Snowflake's systems; however, after receiving legal pressure from Snowflake, it removed its online report.[101]

Snowflake's actions injured Plaintiffs and Class Members.

135. Snowflake's breach of its duty of care and engagement in unfair trade practices caused injury to Plaintiff and Class Members, as discussed herein.

136. Snowflake is liable for the injuries suffered by each Plaintiff and Class Member by virtue of its role as a data storage provider that stored, and failed to protect, the data of all the Spokes.

137. To avoid duplication and for organizational purposes, this section incorporates by reference the following sections that allege in detail the injuries

---

99 Hudson Rock Report, *supra*.

100 *Id.* According to Hudson Rock, the threat actor used a Snowflake employee's work credentials using info-stealing malware to exfiltrate data from Snowflake's customer cloud accounts.

101 Jessica Lyons, *Hudson Rock yanks report fingering Snowflake employee creds snafu for mega-leak*, The Register (Jun 4, 2024), https://www.theregister.com/2024/06/04/snowflake_report_pulled/.

suffered by Plaintiffs and Class Members: Part One, Section III; Part Three, Section VI; Part Four, Section V; Part Five, Section V; and Part Six, Section IV.

CLASS ACTION ALLEGATIONS AS TO SNOWFLAKE.

138. Plaintiffs bring this action on their own behalf, and on behalf of the following Class and Subclasses (referred to collectively as the "Snowflake Classes"):

- **Nationwide Snowflake Class.** All individuals residing in the United States whose Personal Information was identified as compromised in the Data Breach by a Spoke Defendant.
- **State-Specific Subclasses.** As described in this Section below, all individuals residing in a specific state whose Personal Information was identified as compromised in the Data Breach by a Spoke Defendant.

139. Plaintiffs' proposed class definitions against Snowflake are inclusive of proposed national and state class definitions against the Spokes.

140. Excluded from the Snowflake Classes are Snowflake's officers and directors, any entity in which Snowflake has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Snowflake. Excluded also from the Snowflake Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

141. Plaintiffs reserve the right to amend or modify the definition of the Snowflake Classes or create additional subclasses as this case progresses.

142. **Numerosity.** The members of the Snowflake Classes are so numerous that joinder of all of them is impracticable. Public reporting presently indicates that there are hundreds of millions of individuals whose Personal Information was stored on Snowflake's Data Cloud and exfiltrated in the Data Breach.

143. **Commonality.** There are questions of fact and law common to the Snowflake Classes, which predominate over individualized questions. These common questions of law and fact include, but are not limited to:

- Whether Snowflake had a duty to protect the Personal Information of Plaintiffs and Snowflake Class Members, and whether it breached that duty.
- Whether Snowflake knew or should have known that its data security practices were deficient.
- Whether Snowflake's data security systems were consistent with industry standards prior to the Data Breach.
- Whether Snowflake's failure to require customers to implement MFA, employ credential rotation, and employ other industry standard data security measures violated a standard of care or laws.
- Whether Plaintiffs and Snowflake Class members are entitled to actual damages, punitive damages, treble damages, statutory damages, nominal damages, general damages, and/or injunctive relief.

144. **Typicality.** Plaintiffs' claims are typical of those of other Snowflake Class members because the Plaintiffs' Personal Information, like that of every other Snowflake Class Member, was compromised in the Data Breach

145. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interest of the Snowflake Class members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

146. **Predominance.** Snowflake engaged in a common course of conduct toward the Plaintiffs and Snowflake Class members, in that their data was stored on the same Snowflake Data Cloud network and unlawfully accessed in the same manner. The common issues arising from Snowflake's conduct affecting Class Members listed above predominate over any individualized issues. Adjudication of these common issues in a single action will advance judicial economy.

147. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the claims of the Snowflake Classes. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Snowflake Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Snowflake Class members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Snowflake. In contrast, conducting this action as a class action presents far fewer management

difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Snowflake Class Member.

148. **Injunctive Relief.** Snowflake has acted on grounds that apply generally to the Snowflake Classes as a whole such that class certification, injunctive relief, and declaratory relief are appropriate on a class-wide basis.

149. **Issue Certification.** Likewise, certain issues are appropriate for certification because such claims present common issues whose resolution would advance the disposition of this matter. Such issues include, but are not limited to:

- Whether Snowflake owed a legal duty to Plaintiffs and Snowflake Class members to protect their Personal Information.
- Whether Snowflake's data security measures were inadequate in light of applicable regulations and industry standards.
- Whether Snowflake's data security measures were negligent or reckless.

150. **Identification of Class Members via Objective Criteria.** Finally, all members of the proposed Snowflake Classes are readily identifiable using objective criteria. Both Snowflake and the Spokes have access to the names and contact information of Snowflake Class members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by the Spokes.

FIRST CLAIM FOR RELIEF
Negligence
On behalf of All Plaintiffs and the Nationwide Snowflake Class

151. Plaintiffs repeat and re-allege the allegations contained in the foregoing paragraphs as set forth fully herein.

152. Snowflake owed a duty under common law to Plaintiffs and Nationwide Snowflake Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, and deleting their Personal Information in its possession from being compromised, stolen, or misused by unauthorized persons.

153. Specifically, this duty included, among other things: (a) implementing industry standard data security safeguards to protect the Personal Information of Plaintiffs and Nationwide Snowflake Class members relating to MFA, rotating credentials, and restricting access privileges; (b) maintaining, testing, and monitoring Snowflake's security systems to ensure that Personal Information was adequately secured and protected; and (c) implementing intrusion detection systems and notifying customers of suspicious intrusions.

154. Snowflake's duty to use reasonable care arose from several sources, as described herein, including that Snowflake knew or should have known that the information it stored for the Spokes was sensitive, and that failing to take adequate steps to secure and protect the data would foreseeably lead to a Data Breach which could injure individual consumers.

155. Snowflake had a common law duty to prevent foreseeable harm to others. This duty existed because Snowflake stored valuable Personal Information that is routinely targeted by cyber criminals. Plaintiffs and Nationwide Snowflake Class members were the foreseeable and probably victims of any compromise to inadequate data security practices maintained by Snowflake.

156. Snowflake further assumed a duty of reasonable care in making representations in marketing materials that their data storage services were secure and offered "built-in" and turnkey solutions for data security compliance.

157. Snowflake breached its duty owed to the Plaintiffs and Nationwide Snowflake Class members by failing to maintain adequate data security practices that conformed with industry standards, and were therefore negligent.

158. But for Snowflake's negligence, the Personal Information of the Plaintiffs and Nationwide Snowflake Class members would not have been stolen by cybercriminals in the Data Breach.

159. As a direct and proximate result of Snowflake's breach of its duties, Plaintiffs and Nationwide Snowflake Class members have suffered injuries as detailed herein.

160. As a direct and proximate result of Snowflake's negligence, Plaintiffs and Nationwide Snowflake Class members are entitled to damages, including

compensatory, punitive, nominal damages, and/or general damages in an amount to be proven at trial.

SECOND CLAIM FOR RELIEF
Violation of the Montana Unfair Trade Practices & Consumer Protection Act (Mont. Code Ann. § 30-14-101, *et seq.*) ("MUTPCPA")
On behalf of All Plaintiffs and the Nationwide Snowflake Class

161. Plaintiffs repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Two, as set forth fully herein.

162. Plaintiffs and Nationwide Snowflake Class members are "consumers" under the MUTPCPA because they purchased ticketing services for personal, family, or household purposes. Mont. Code Ann. § 30-14-102(1).

163. Snowflake is a "person[]" under the MUTPCPA, which is defined to mean "natural persons, corporations, trusts, partnerships, incorporated or unincorporated associations, and any other legal entity." Mont. Code Ann. § 30-14-102(6).

164. Snowflake engaged in "trade" and "commerce" as defined by the MUTPCPA because it operates its data cloud services and makes decisions regarding data security from its Montana headquarters. Mont. Code Ann. § 30-14-102(8)(a) (defining "trade" and "commerce" to mean the "sale, or distribution of any services . . . tangible or intangible . . . wherever located, and includes any trade or commerce directly or indirectly affecting the people of this state"). The State of

Montana has a compelling interest in ensuring that companies within its jurisdiction follow its laws.

165. Snowflake engaged in unfair trade practices prohibited by the MUTPCPA. Mont. Code Ann. § 30-14-103.

166. Snowflake engaged in unfair trade practices when it failed to maintain reasonable data security practices to safeguard the Personal Information of Plaintiffs and Snowflake Class members, as described herein.

167. Snowflake's conduct offends established public policy and is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers.

168. Montana has the most significant relationship with Snowflake's unfair trade practices alleged herein such that it is proper to apply the MUTPCPA to the Nationwide Snowflake Class. Snowflake is headquartered in Montana. As Snowflake made decisions regarding the data security policies and practices that are challenged in this action from its Montana headquarters, the conduct causing Plaintiffs' and Class members' injury occurred in Montana. Finally, Montana has a strong interest in regulating the trade practices of companies headquartered within its borders.

169. Plaintiffs and Snowflake Class members have suffered injury as a result of Snowflake's unfair trade practices, as described herein.

170. As a direct and proximate result of Snowflake's unfair trade practices, Plaintiffs and Snowflake Class members are entitled to injunctive relief, damages, including actual damages in an amount to be proven at trial or statutory damages of $500, whichever is greater, treble damages of actual damages, and reasonable attorneys' fees. Mont. Code Ann. § 30-14-133.

RESERVATION OF RIGHTS TO ASSERT ADDITIONAL CLAIMS FOR RELIEF

171. Plaintiffs have asserted claims in this complaint in order to confer subject matter jurisdiction over Defendants so that this case may be transferred to the District of Montana by the Judicial Panel on Multidistrict Litigation.

172. To the extent this case is transferred back to this Court for trial, Plaintiffs reserve the right to assert additional causes of action or amend their causes of action as applicable and based upon discovery and motion practice in the MDL

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes set forth herein, respectfully request the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are the proper class representatives; and appoint Plaintiff's counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit and prevent Snowflake from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiffs and Class Members compensatory, consequential, general, and/or nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court award punitive or exemplary damages, to the extent permitted by law;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Snowflake as a result of its unlawful acts, omissions, and practices;

F. That Plaintiff be granted the declaratory and injunctive relief to prevent further injuries from manifesting as alleged herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper; and

I. Any other relief that the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial in the instant action.

Dated: February 3, 2025

Respectfully submitted by:

/s/ Raphael Graybill
Raphael Graybill
Graybill Law Firm, PC
300 4th Street North
Great Falls, MT 59401
Tel. 406.452.8566
raph@graybilllawfirm.com

Amy Keller
DiCello Levitt LLP
Ten North Dearborn, Sixth Floor
Chicago, Illinois 60602
Tel. 312.214.7900
akeller@dicellolevitt.com

Jason S. Rathod
Migliaccio & Rathod LLP
412 H St NE, Suite 302
Washington DC 20002
Tel. 202.470.3520
jrathod@classlawdc.com

John Heenan
Heenan & Cook
1631 Zimmerman Trail
Billings, MT 59102
Tel. 406.839.9091
john@lawmontana.com

J. Devlan Geddes
Goetz, Geddes & Gardner P.C.
35 N. Grand Ave.
Bozeman, MT 59715
Tel. 406.587.0618
devlan@goetzlawfirm.com

Counsel for Plaintiffs and the Putative Class